基于LDAP的PKI证书的存储与备份

何朝辉 李 琦 卿斯汉

（中国科学院软件研究所 北京100080）（中国科学院信息安全技术工程研究中心 北京100080）

摘 要 本文较深入地介绍了LDAP协议在PKI体系中的应用，主要讲述了如何利用LDAP服务器存储以及备份电子证书。首先简单阐明了目录服务的优点，然后根据存储的需要自定义了LDAP中的属性，并扩展了一个对象类，最后描述了LDAP服务的复制和均衡负载模型。

关键词 LDAP，电子证书，模式，属性，对象类，复制

Storage and Backup of PKI's Certificate Based on LDAP

HE Zhao-Hui LI Qi QING Si-Han

(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

(Engineering Research Center for Information Security Technology, Chinese Academy of Sciences Beijing 100080)

Abstract This article introduces the application of LDAP in PKI system, and describes mainly how to utilize LDAP server to store and back up the electronic certificate. First, some excellencies of directory services are presented. Secondly, according to the needs of certificate's storage, define the attribute of LDAP by oneself, and expand the objectclass. Finally, describe the models of LDAP server's replication and referrals.

Keywords LDAP, Certificate, Schema, Attributetype, Objectclass, Replication

1 引言

PKI(Public Key Infrastructure)即"公共密钥体系"，提供公钥加密和数字签名服务。其主要目的是通过自动管理密钥和标记个人身份的电子证书，可以为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。

在PKI体系中电子证书是用来存储个人的公私钥对以及其他一些需要的个人信息，是用来标记个人身份的关键。如果因为病毒破坏、物理损坏、他人攻击而导致证书的丢失，其损失是巨大的，故证书的存储、备份是极其重要的。一般用来存储证书有三种方式，一种是使用文件型数据库，如Berkeley DB；一种是使用关系型数据库，如MySQL、DB2、SQL Server之类的；还有一种是基于目录服务的，利用目录服务器存储备份。

Berkeley DB是一种文件型数据库，它提供一种基于硬盘的可扩展的Hash算法，可以很有效的方式将"键-值"存储到硬盘或者从硬盘读取。但它直接支持的操作很少，只有"add data where key = x"和"select data where key = x"，并不适合于存储电子证书这样复杂的数据类型，而且缺乏安全性，也不方便审计[1]。

关系型数据库(RDBMS)，现在数据库产品的主流，其以行和列组成表，用表来存储数据，以关系来组织各数据项，一组表便成了数据库。它可以很方便地用来存储各种数据，但对电子证书这种写入很少而查询比较频繁的数据类型并没有特别优化，效率上可能显得不太高。

目录服务是一种特殊的数据库系统，可以用来保存描述性的、基于属性的信息，并且支持复杂的过滤搜索能力。其专门针对读取、浏览和搜索操作进行了特定的优化，当从目录服务器中读取数据的时候会比没有对读取查询进行专门优化的关系型数据库中读取数据快一个数量级。另外，它们可以具有大范围复制信息的功能，以便提高可用性和可靠性，同时缩短响应时间。基于以上优点本文利用目录服务进行证书的存储与备份，其具体使用的协议是LDAP(轻量级目录访问协议)。

2 LDAP的简介

LDAP的英文全称是Lightweight Directory Access Protocol，现在是第3版，简称为LDAPv3。它是基于X.500标准的，但是简单多了并且可以根据需要定制。而且与X.500不同的是LDAP支持TCP/IP，这对访问Internet是必须的。

LDAP协议所采用的总体模型是某个客户端(client)通过服务器(server)执行协议操作。在此模型中，客户端传送一个协议请求来描述将被服务器执行的操作，服务器负责在目录中执行必要的操作。在完成了操作后，服务器返回一个包含结果或错误信息的响应至客户端。虽然服务器需要返回响应，但并不需要同步。对于多个操作的请求和响应，客户端和服务器端可以以任何顺序进行交换，只要每个客户端的请求最终都得到必要的响应即可。如图1所示，客户端送出请求1和请求2后才收到响应，而且请求3的响应在请求2的之前[2,3]。

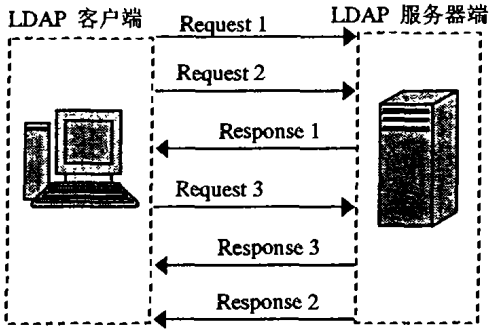

图1 LDAP的请求与响应

何朝辉 硕士，研究方向为PKI/CA、蠕虫病毒；李 琦 工程师；卿斯汉 研究员，博士生导师，研究方向为大型网络信息安全技术。

大多数 LDAP 服务器都为读密集型的操作进行专门的优化，所以比较适合于存储修改较少、查询较多的数据，比如，客户的联系信息、软件包的配置信息、公司员工的名片以及公用证书和安全密钥等等。其数据是以树状的层次结构存储的，类似于自顶向下的 DNS 树或 UNIX 文件的目录树，在“证书的存储”这节中有具体描述[4]。

LDAP 服务器可以用于存储各种不同的数据类型，通过服务器发布的模式(schema)支持不同的语法、匹配规则、属性类型和对象类，并且可以按照 RFC 中 schema 的定义根据需求对模式文件进行扩展，从而支持其他的语法，匹配规则，属性类型和对象类。在“证书的存储”这节中我们会扩展一个相对简单的模式文件。

LDAP 提供了访问控制实例 ACI(access control instances)，可以在服务器端控制这些访问，这比用客户端的软件保证数据的安全可安全得多。用 LDAP 的 ACI，可以在很小的粒度上对创建者、管理员、用户、过客的权限进行控制，从而很好地保证了 LDAP 服务器中数据的安全性。

基于以上优点，利用 LDAP 服务器作为电子证书的存储服务器和备份服务器是非常合适的。在整个 PKI 体系中证书的管理是非常重要的，其涉及到证书的申请、审核、发布、撤销、存储、备份，图2展示了一个证书管理的体系结构[5]。其中 RA(Registration Authority)负责对申请者提供的申请资料及申请资格进行审核，以决定是否同意为该申请者签发证书。CA(Certificate Authority)用于颁发、撤消证书。

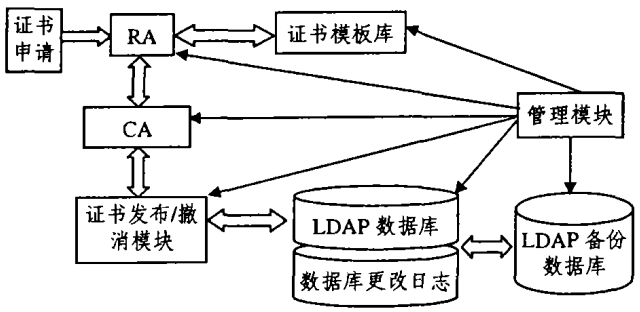

图2 证书服务器体系结构

LDAP 协议是一种开放的、跨平台的协议，很多厂商都在其产品中集成了对 LDAP 的支持，而且无论是商业平台还是开源平台，都有很多 LDAP 服务器。比如 IBM 的 SecureWay、CA 公司的 eTrust Directory、微软的活动目录，以及开源世界里面最著名的 OpenLDAP。在本文中，使用的是开放源代码的 OpenLDAP，现在的最新版本是2.2.7版，可以从其官方网站 www.openldap.org 下载。

3 证书的存储

LDAP 目录中的信息是按照树型结构组织，具体信息存储在条目(entry)的数据结构中。条目相当于关系数据库中表的记录；条目是具有区别名 DN(Distinguished Name)的属性(Attribute)，DN 是用来引用条目的，DN 相当于关系数据库表中的关键字(Primary Key)。属性由类型(Type)和一个或多个值(Values)组成，相当于关系数据库中的字段(Field)由字段名和数据类型组成，只是为了方便检索的需要，LDAP 中的 Type 可以有多个 Value，而不是关系数据库中为降低数据的冗余性要求实现的各个域必须是不相关的。LDAP 中条目的组织一般按照地理位置和组织关系进行组织，非常地直观。作为一个例子，以下是一个简单的目录设计图，如图3所示[2,6,7]。

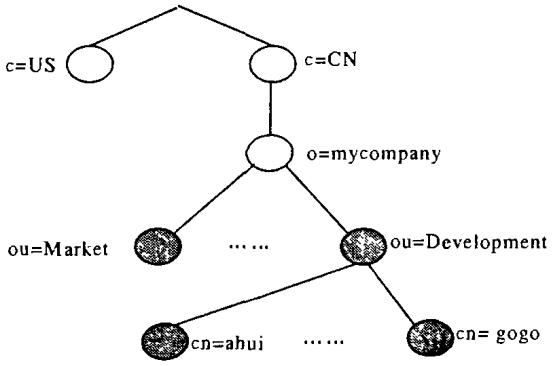

图3 目录设计图

用户 ahui 的证书在 LDAP 数据库中的逻辑位置就是 DN：cn＝ahui，ou＝Development，o＝mycompany，c＝CN，这相当于关系数据库中的关键字，其值就是用户的数字证书。

在 LDAP 中用模式(schema)来说明目录可以用来支持的语法，匹配规则，属性类型和对象类，我们可以根据自己的需要扩展基本的 LDAP 目录的功能，创建新的对象类或者扩展现存的对象类。为了更方便地存储证书，我们可以定义一个新的属性，并且扩展一个现存的对象类。属性定义如下[6,8]：

```
attributetype (1.1.2.1.1
NAME'MyCertificate'
DESC' Certificate'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.8
SINGLE-value)
```

在 LDAP 协议中，属性定义采用关键字、属性代号、属性名、属性语法(属性值应满足的约束条件)的格式。在上面的属性定义中，1.1.2.1.1是一个全局唯一对象标识符(OID)，可以向 IANA(Internet Assigned Numbers Authority)维护的 Private Enterprise arch 下申请一个 OID。任何私人企业或者组织可以申请一个在此 arch 下的 OID。只需要填写一个位于 http://www.iana.org/cgi-bin/ enterprise.pl 的 IANA 表单就可以了，您的合法 OID 将在几天内发送给您。NAME 是表示属性的名字，DESC 是说明，SYNTAX 属性语法，在 RFC2522中定义证书的类型是1.3.6.1.4.1.1466.115.121.1.8，SINGLE-value 表示单值属性。

随后以对象类 inetOrgPerson 为父类建一个新的对象类 myCertObject，其的定义如下[6,9]：

```
objectclass ( 1.1.2.2.1
        NAME' myCertObject'
        DESC' Certificate'
        SUP inetOrgPerson
        MUST MyCertificate )
```

在上面对象类的定义中1.1.2.2.1和属性定义中的相似，都是全局唯一对象标识符(OID)，由 IANA 颁发，DESC 是说明，SUP 是继承的父类，子类继承父类的各种属性项，包括可选项和必须项。MUST 是所定义的对象类 myCertObject 必须有的属性。

定义好对象类后，创建新的 schema，将属性和对象类的定义写入，并被包含在 OpenLDAP 的配置文件 slapd.conf 中。随后重新启动 OpenLDAP，就可以用来存储证书了。

4 证书的备份

在 LDAP 服务器中数据的复制是很容易实现的，但复制技术并没有形成标准，也缺少相应的 RFC 文档，各个不同的 LDAP 服务器有不同的复制实现方法。OpenLDAP 中的复制技术来自于密歇根州立大学(University of Michigan)的 LDAP 服务器，其实现方法是：利用一个后台程序 slurpd 监

视主 LDAP 服务器的日志文件，发生改变时 slurpd 就通知从 LDAP 服务器，让其同步。本文图4中显示了主 LDAP 中 slapd、slurpd 和从 LDAP 中 slapd 的关系[2]。

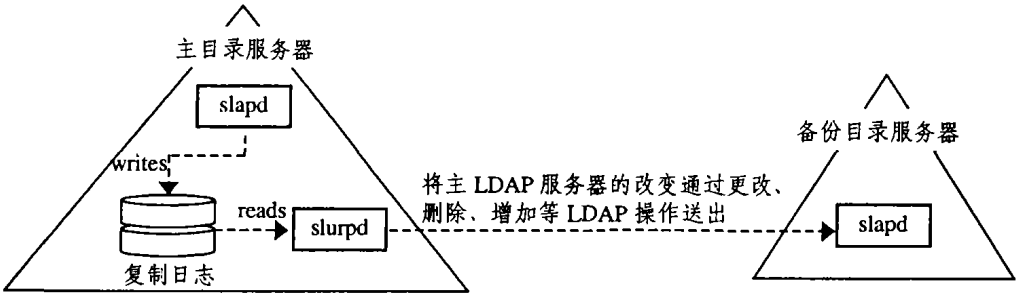

图4　主从 LDAP 服务器复制示意图

slurpd 提供了从主 slapd 向附属 slapd 实例传播改变的能力。这种主/附属安排提供了一个简单有效的方法来提高服务容量、可用性和可靠性。以下是一个 LDAP 的修改操作过程：

①LDAP 客户端向主 slapd 提交 LDAP 修改请求操作；

②主 slapd 执行修改请求，将改变写入复制日志文件，然后给客户端返回一个成功代码；

③slurpd 进程注意到一个新的条目附加到复制日志文件，读取该复制日志条目，然后通过 LDAP 将改变发送给从属 slapd；

④从属 slapd 执行修改操作，给 slurpd 进程返回一个正确的代码。

更改 OpenLDAP 的配置文件 slapd.conf，允许产生复制日志文件，则复制日志给出了复制站点，一个时间戳，被修改的 DN 的条目，以及指明了所发生的改变的多行信息。这样通过查看日志文件，管理员可以很方便地审核、查看主从服务器的变动内容。

也可以设立一个主服务器和一个或多个附属服务器，让这些服务器都参与查询，在它们中间分布负载。这样当有大量的通过 LDAP 来请求目录服务的操作致使主服务器繁忙，则主服务器可以向客户端返回附属服务器的地址，让客户端向附属服务器请求 LDAP 操作，并返回一个成功代码，从而达到负载均衡的目的。图5展示了一个在目录结构内部如何实现负载均衡[10]。

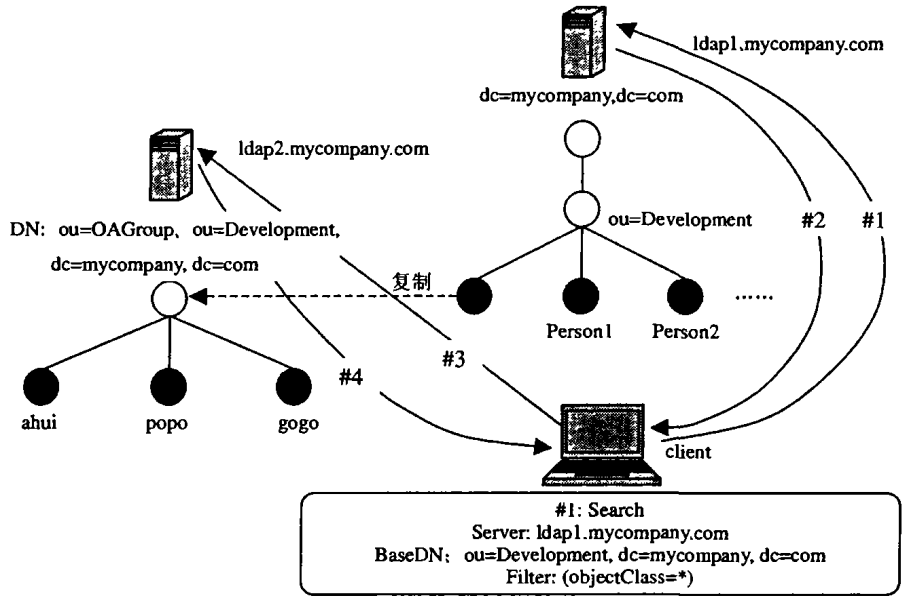

图5　负载均衡的实现

结论　LDAP 协议是一种跨平台、标准并且开放的协议，各类应用软件可以很方便地加入对 LDAP 的支持；而且其安全性、查询效率、容错能力都是非常不错的，自然 LDAP 的使用也越来越广泛，包括邮件系统、证书系统、电子商务中的客户信息系统等等。基于 LDAP 的这些优点，相信会有更多以查询为主的系统越来越倾向于 LDAP 的使用。

参 考 文 献

1 Gutmann P. A Reliable, Scalable General-purpose Certificate Store. http://www.cypherpunks.to/~peter/09a-cert-store.pdf, 2001

2 Carter G. LDAP System Administration Gera ld Carter. USA: O'Reilly, Mar. 2003

3 Wahl M, Howes T, Kille S. Lightweight Director y Access Protocol (v3). RFC2251. http://www.ietf.org/rfc/rfc2251.txt, Dec. 1997

4 Donnelly M. An Introduction to LDAP. http://www.ldapman.net/articles/index.html, Apr. 2000

5 汤素锋，潘雪增，平玲娣. 基于 LDAP 协议的独立证书服务器的设计与实现. 见：第三届中国信息和通信安全学术会议(CCICS'2003). 武汉大学. Mar. 2003

6 The OpenLDAP Project. OpenLDAP 2.2 Administ rator's Guide. http://www.openldap.org/doc/admin22, Feb. 2004

7 Good G. The LDAP Data Interchange Format (LD IF) - Technical Specification. RFC2849. http://www.ietf.org/rfc/rfc2849.txt, Jun. 2000

8 Wahl M, Coulbeck A, Howes T, Kille S. Lightw eight Directory Access Protocol (v3): Attribute Syntax Definitions. RFC2252. http://www.ietf.org/rfc/rfc2252.txt. Dec. 1997

9 Smith M. Definition of the inetOrgPerson LDAP Object Class. RFC 2798. http://www.ietf.org/rfc/rfc2798.txt. Apr. 2000

10 Arkills B. LDAP Directories Explained. USA: Addison Wesley, Feb. 2003